International Journal of Security and Its Applications
Vol.9, No.2 (2015), pp.189-202
http://dx.doi.org/10.14257/ijsia.2015.9.2.18

An efficient ID-based Beta Cryptosystem

Chandrashekhar Meshram

Department of Mathematics
RTM Nagpur University, Nagpur, India
cs_meshram@rediffmail.com

Abstract

In 1984, Shamir [1] introduced the concept of an identity-based cryptosystem. In this system, each user needs to visit a public key generation (PKG) and identify himself before joining a communication network. Once a user is accepted, the PKG will provide him with a secret key. In this way, if a user wants to communicate with others, he only needs to know the "identity" of his communication partner and the public key of the PKG. There is no public file required in this system. However, Shamir did not succeed in constructing an identity based cryptosystem, but only in constructing an identity-based signature scheme. Meshram and Meshram [5] have proposed an identity-based beta cryptosystem, security under the generalized discrete logarithm problem with distinct discrete exponents in the multiplicative group of finite fields and integer factorization problem.

In this paper, we propose some modification in identity-based beta cryptosystem based on generalized discrete logarithm problem with distinct discrete exponents in the multiplicative group of finite fields and integer factorization problem and we consider the security against a conspiracy of some entities in the proposed system and show the possibility of establishing a more secure system.

Keywords: *Public key Cryptosystem, Identity based Cryptosystem, Discrete Logarithm Problem (DLP), Generalized Discrete Logarithm Problem (GDLP), Beta Cryptosystem and Integer Factorization Problem (IFP)*

1. Introduction

In an open network environment, secret session key needs to be shared between two users before it establishes a secret communication. While the number of users in the network is increasing, key distribution will become a serious problem. In 1976, Diffie and Hellman [4] introduced the concept of the public key distribution system (PKDS). In the PKDS, each user needs to select a secret key and compute a corresponding public key and store in the public directory. The common secrete session key, which will be shared between two users can then be determined by either user, based on his own secret key and the partner's public key. Although the PKDS provides an elegant way to solve the key distribution problem, the major concern is the authentication of the public keys used in the cryptographic algorithm.

In 1984, Shamir [1] introduced the concept of an identity. In this system, each user needs to visit a public key generation (PKG) and identify himself before joining the network. Once a user's identity is accepted, the PKG will provide him with a secret key. In this way, a user needs only to know the "identity" of his communication partner and the public key of the PKG, together with his secret key, to communicate with others. There is no public file required in this system. However, Shamir did not succeed in constructing an identity-based cryptosystem, but only in constructing an identity-based signature scheme. Since then, much research has been devoted, especially in Japan, to various kinds of identity-based cryptographic schemes. Okamoto *et al.*, [6] proposed an

ISSN: 1738-9976 IJSIA

identity-based key distribution system in 1988, and later, Ohta [10] extended their scheme for user identification. These schemes use the RSA public key cryptosystem [14] for operations in modular N, where N is a product of two large primes, and the security of these schemes is based on the computational difficulty of factoring this large composite number N. Tsujii and Itoh [2] have also proposed an identity-based cryptosystem based on the discrete logarithm problem with single discrete exponent which uses the ElGamal public key cryptosystem.

In 1991, Maurer and Yacobi [22] developed a non-interactive identity-based public-key distribution system. In their scheme, the public keys are self-authenticated and require no further authentication by certificates. However, some problems with this scheme were found, the scheme was modified and the final version was presented [23]. In 1998, Tseng and Jan [24] improved the scheme proposed by Maurer and Yacobi, and provided a non-interactive identity-based public-key distribution system with multi-objectives such as an identity-based signature scheme, an identification scheme, and a conference key distribution system. In their scheme, the computational complexity of the system is heavy. Therefore, it is necessary to have a powerful computational capability. L. Harn [13] proposed public key cryptosystem design based on factoring and discrete logarithm whose security is based factoring and discrete logarithm. In 2001, Boneh and Franklin, Cocks [25] used a variant of integer factorization problem to construct his identity-based encryption scheme. However, the scheme is inefficient in that a plain-text message is encrypted bit-by-bit and hence the length of the output ciphertext becomes long.

In 2004, Wei Bin Lee & Kuan Chieh Liao [8] design a transformation process that can transfer all of discrete logarithm based cryptosystems into the identity-based systems rather than reinvent a new system. After 2004 several identity-based cryptosystems [9, 15, 18, 19, 20, 21, 33-38] have been proposed. But in these schemes, the public key of each entity is not only an identity, but also some random number selected either by the entity or by the trusted authority. In 2009 Mihir Bellare *et al.*, [11] provides security proof or attacks for a large number of identity-based identification and signature schemes. Underlying these is a framework that on the one hand helps explain how these schemes are derived and on the other hand enables modular security analyses, thereby helping to understand, simplify, and unify previous work. In 2010 Chandrashekhar Meshram [16] has also proposed Cryptosystem based on double generalized discrete logarithm problem whose security is based on double generalized discrete logarithm problem with distinct discrete exponents in the multiplicative group of finite fields. After some time Chandrashekhar Meshram presented the modification of identity-based cryptosystem based on the double discrete logarithm problem [17, 7] and also proposed an Identity based beta cryptosystem, whose security is based on generalized discrete logarithm problem and integer logarithm problem [5].

Based on the observation that new cryptographic schemes always face security challenges and confidentiality concerns and many integer factorization & discrete logarithm-based cryptographic systems have been deployed. The major contribution of our scheme is the key generation phase, which is just a simple transformation process with low computational complexity. No modification of the original design of the discrete logarithm and integer factorization based cryptosystems is necessary. Therefore, the new scheme has the same security as the original one, and retains all of the advantages of the identity-based cryptosystem.

In this paper, we propose some modification in identity-based beta cryptosystem based on generalized discrete logarithm problem with distinct discrete exponents in the multiplicative group of finite fields and integer factorization problem (the basic idea of the proposed system comes on the public key cryptosystem based on generalized discrete logarithm problem and integer factorization problem) here we describe further considerations such as the security of the system, the identification for senders. etc. our scheme does not require any interactive preliminary communications in each message

transmission and any assumption except the intractability of the discrete logarithm problem. (this assumption seems to be quite reasonable) thus the proposed scheme is a concrete example of an identity-based cryptosystem which satisfies Shamir's original concept [1] in a strict sense.

2. Modified Identity-based Cryptosystem

2.1. Preparation for the Center and Each Entity

Step 1: Each user generates a k-dimensional binary vector for his ID. We denote user $i's$ ID by ID_i as follows:

$$ID_i = (x_{i1}, x_{i2}, x_{i3}, \ldots\ldots\ldots, x_{ik}), x_{ij} \in \{0,1\}, (1 \le j \le k) \quad (1)$$

Each user registers his ID with the center, and the center stores it in a public file.

Step 2: The center generates random two arbitrary large prime numbers p and q, and computes

$$N = p * q \quad (2)$$

Then the center chooses an arbitrary random number e satisfying $\gcd(e, \varphi(N)) = 1$, where $\varphi(N) = (p-1)(q-1)$ is the Euler function of N then center publishes (e, N) as the public key. Any user can compute the user $i's$ extended ID, EID_i by the following:

$$EID_i = (ID_i)^e \pmod{N}$$

$$= (y_{i1}, y_{i2}, y_{i3}, \ldots\ldots\ldots, y_{it}), y_{ij} \in \{0,1\}, (1 \le j \le t) \quad (3)$$

where $t = |N|$ is the number of bits of N.

Step 3: ***Center's secrete information:*** The center generates n-dimensional vector $\vec{a}$ over $Z^*_{\varphi(N)}$ which satisfies:

$$\vec{a} = (a_1, a_2, a_3, \ldots\ldots\ldots, a_n), 1 \le a_i \le \varphi(N), (1 \le i \le n) \quad (4)$$

$$aI \ne aJ \pmod{N}, I \ne J \quad (5)$$

Where I and J are n-dimensional binary vector and stores it as the centers secret information. The condition of equation (5) is necessary to avoid the accidental coincidence of some users secrete keys. A simple way to generate the vector $\vec{a}$ is to use the Merkle and Hellman scheme [12].

Step 4: The center also chooses w which satisfies $\gcd(w, \varphi(N)) = 1$ and $w \prec \lfloor \varphi(N)/n \rfloor$, where $\lfloor x \rfloor$ denote the floor function which implies the largest integer smaller than compute x.

The center chooses a super-increasing sequence corresponding to a as $a'_i (1 \le i \le n)$

satisfies $\sum_{j=1}^{i-1} a'_j + v \prec \varphi(N)$ where $v = \lfloor \varphi(N)/w \rfloor$ (6)

$$\sum_{j=1}^{n} a'_j \prec \varphi(N) \quad (7)$$

Then the centre computes

$$a_i = a' w (\text{mod } \varphi(N))$$

$$c_i = a_i (\text{mod } w)(1 \le i \le n) \quad (8)$$

Step 5: The center also chooses a unique integer d , $(1 \le d \le \varphi(N))$ such that $ed \equiv 1(\text{mod } \varphi(N))$, and t arbitrary integers $(e_1, e_2, e_3, \ldots\ldots, e_t)(1 \le t \le n)$,satisfying $\gcd(e_t, \varphi(N)) = 1$ and compute n-dimensional vectors D^j respectively:

$$D^j = (d_1^j, d_2^j, d_3^j, \ldots\ldots, d_n^j)(1 \le j \le n)$$

$$d_l^j = e_l a_l (\text{mod } \varphi(N))(1 \le l \le n) \quad (9)$$

Since D^j is one to one system.

Step 6: ***Center public information:*** The center chooses an arbitrary element β of Z_N^* and computes n-dimensional vector h using element β corresponding to the vector.

$$h = (h_1, h_2, h_3, \ldots\ldots, h_n) \quad (10)$$

$$h_i = \beta^{a_i} (\text{mod } N), (1 \le i \le n) \quad (11)$$

The center informs each user (N, e, h) as public information.

Step 7: ***Each user secrete key:*** User $i's$ secrete keys s_i is computed by inner product of a with the condition $d_l^j = e_l a_l (\text{mod } \varphi(N))(1 \le l \le n)$ (the centre's secret information) and EID_i (entity $i's$ extended ID, see eqn.3)

$$s_i = d_l^j EID_i (\text{mod } \varphi(N))$$

$$= \sum_{1 \le j \le n} d_l^j y_{ij} (\text{mod } \varphi(N)) \quad (12)$$

3. Protocol of the Proposed Cryptosystem

Without loss of generality, we suppose that user 2 sends message M to user 1.

Encryption

User 2 generates EID_1 (User $i's$ extended ID, see equation 3) from ID_1. It then computes γ_1 from corresponding public information h and EID_1 :

$$\gamma_1 = \prod_{1 \le i \le n} (h_i^{y_{1i}})^{e_i} (\text{mod } N)$$

$$= \prod_{1 \le i \le n} ((\beta^{a_i})^{y_{1i}})^{e_i} (\text{mod } N)$$

$$= \beta^{\sum_{1 \le i \le n} d_l^j y_{1i} \pmod{\varphi(N)}} \pmod{N}$$

$$= \beta^{s_1} \pmod{N} \quad (13)$$

User 2 will use γ_1 in our proposed scheme.

Let $M (1 \le M \le N-1)$ a message to be transmitted by user 2 select a random integer e such that $\gcd(e, \varphi(N)) = 1$ and computes cipher text as follows:

$$C = (M \beta^{s_1})^e \pmod{N} \quad (14)$$

Decryption

To recover the plaintext M from the cipher text
User 1 does the following :
User 1 sends the cipher text C to user 2 via an insecure channel, when user 2 receives the cipher text, he computes

$$y_2 = \beta^{\varphi(N)-s_1} \pmod{N} = \beta^{-s_1} \pmod{N} \quad (15)$$

$$(y_2)^e \pmod{N} = (\beta^{-s_1})^e \pmod{N} \quad (16)$$

Using his secrete key s_1, recovered user 2's the message M by equations. (15) and (16) to compute

$$((y_2)^e * C)^d \pmod{N} = (\beta^{-s_1 e} M^e \beta^{s_1 e})^d \pmod{N}$$

$$= M^{ed} \pmod{N} = M \pmod{N}$$

4. Security Analysis and Discussions

The security of identity-based cryptosystem based on the index problem in the multiplicative cyclic group Z_N^*, where $N = p * q$ (The factorization of N is known only to the center.) where $\varphi(N)$ Euler function of N. In this system Coppersmith showed an attacking method [26] such that $(n+1)$ user's conspiracy can derive the center's secret information.

4.1. Conspiracy of Some Users

1. Center's Secret Information:

The proposed system can accommodate up to 2^k users. Here, consider the case where $m (\succ n)$ users $i, (1 \le i \le m)$ conspire to derive the center's secret information d^j. Each user $i, (1 \le i \le m)$ has partial information of d^j in the following form:

$$d^j_{EID_i} = s_i \pmod{\varphi(N)}, (1 \le i \le m) \quad (17)$$

Thus, (18) is a system of linear congruences as follows:

$$\begin{bmatrix} EID_1 \\ EID_2 \\ EID_3 \\ \cdot \\ \cdot \\ EID_n \end{bmatrix} \begin{bmatrix} d_1^j \\ d_2^j \\ d_3^j \\ \cdot \\ \cdot \\ d_n^j \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ \cdot \\ \cdot \\ s_n \end{bmatrix} (\text{mod } \varphi(N)) \tag{18}$$

$$= D \cdot d^j (\text{mod } \varphi(N)) \tag{19}$$

If the matrix D in (20) involves n linearly independent row vectors over $Z_{\varphi(N)}$, then the center's secret information d^j can be uniquely determined by the m users' conspiracy. However, Nakamura *et al.* [32] and Coppersmith [26] suggested that even in the case where matrix D does not involve n linearly independent row vectors over $Z_{\varphi(N)}$, m users $i, (1 \le i \le m)$ can derive $d^{j'}$, which is equivalent to the original center's secret information.

Theorem 1: The $m (\succ n)$ users $i, (1 \le i \le m)$ can derive an n-dimensional vector $d^{j'}$ over $Z_{\varphi(N)}$, which is equivalent to the original center's secret information.

Proof: Since the proposed identity-based cryptosystem is based on the intractability of the generalized discrete logarithm problem and integer factorization, $\varphi(N)$ must have at least one large prime factor. For simplicity, we assume here that $\varphi(N) = 2^c r$ where $c \prec\prec |\varphi(N)|$ and r is prime. Without loss of generality, for some n users $j, (1 \le j \le n)$ among m users $i, (1 \le i \le m)$, we might have the matrix D',

$$D' = \begin{bmatrix} EID_1 \\ EID_2 \\ EID_3 \\ \cdot \\ \cdot \\ EID_n \end{bmatrix} \tag{20}$$

which satisfies $\det D' \neq 0 (\text{mod } r)$. Hence, such n users can derive a' satisfying the following relation:

$$d^{j'} = (d_1^j, d_2^j, d_3^j, \ldots\ldots, d_n^j)$$

$$d^{j'} = d_i^j (\text{mod } r), (1 \le i \le n) \tag{21}$$

An arbitrary users secret key, *e.g.*, user ***k's*** secret key s_k, can be decided by computing $s_k' = EID_k d^{j'} (\text{mod } r)$.

Here, $d^{j'}$ is not necessarily identical to the original user k's secret key s_k; however, the difference between s_i and s_k is some integer multiple of r.Hence, the original user k's secret key s_k can be computed in at most c trials where $\varphi(N) = 2^c r$ and $c \prec\prec |\varphi(N)|$.

Thus, up to $(n-1)$ users never can derive the center's secret information by attack 1; however, more than n users can compute $d^{j'}$, which is equivalent to the center's secret information, and an arbitrary user can be attacked by using $d^{j'}$.

4.2 Each Users Secret Key:

As discussed in Section (V-A-l), up to $(n-1)$ users cannot derive the center's secret information by attack (Theorem 1), while n or more users can compute $d^{j'}$, which is equivalent to the center's secret information. In this subsection, we consider the security of each user's secret key s_i against $t \prec (n)$ user's conspiracy.

When $t \prec (n)$ users conspire, they have the following system of linear congruences:

$$\begin{bmatrix} EID_1 \\ EID_2 \\ EID_3 \\ \cdot \\ \cdot \\ EID_n \end{bmatrix} \begin{bmatrix} d_1^j \\ d_2^j \\ d_3^j \\ \cdot \\ \cdot \\ d_n^j \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ \cdot \\ \cdot \\ s_n \end{bmatrix} (\mathrm{mod}\ \varphi(N)) \tag{22}$$

$$= D''.d^j (\mathrm{mod}\ \varphi(N)) \tag{23}$$

If there exists a t-dimensional vector **c** over $Z_{\varphi(N)}$ such that for an user k

$$c.D'' = \sum_{1 \le i \le t} c_i EID_i (\mathrm{mod}\ \varphi(N)) \tag{24}$$

$$= EID_k (\mathrm{mod}\ \varphi(N)) \tag{25}$$

then $t \prec (n)$ users can compute the user k's secret key s_k by

$$s_k = \sum_{1 \le i \le t} c_i s_i (\mathrm{mod}\ \varphi(N)) \tag{26}$$

Noting that $Z_{\varphi(N)}$ is not a field, it is easily shown that $t \prec (n)$ users ' conspiracy can generate at most 2^t other users ' secret keys as in (35). Hence, the probability that $t \prec (n)$ users can derive another users's secret key is at most $2^t / 2^n = 2^{t-n}$.

Theorem 2 [26]: The $(n+1)$ users' $i, (1 \le i \le n+1)$ can derive an n-dimensional vector $d^{j'}$ over Z_N^* which is equivalent (not necessarily identical) to the original center's secret information.

Proof: when $(n+1)$ users' $i, (1 \le i \le n+1)$ conspire, they have the following system of linear congruences:

$$\begin{bmatrix} EID_1 \\ EID_2 \\ EID_3 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ EID_{n+1} \end{bmatrix} \begin{bmatrix} d_1^j \\ d_2^j \\ d_3^j \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ d_n^j \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ s_{n+1} \end{bmatrix} (\mathrm{mod}\ \varphi(N)) \tag{27}$$

Since each EID_i is an n-dimensional binary vector, there exists an $(n+1)$-dimensional vector c over the integer ring such that

$$\sum_{1 \le i \le n+1} c_i EID_i = 0 \tag{28}$$

Thus we have

$$\sum_{1 \le i \le n+1} c_i s_i = 0 (\mathrm{mod}\ \varphi(N)) \tag{29}$$

And then

$$\sum_{1 \le i \le n+1} c_i s_i = A\varphi(N) \tag{30}$$

If $A \neq 0$,then the $(n+1)$ users can have an integer multiple of $\varphi(N)$ **,** and they can find out the factorization of N .

Then, a similar method with attack (Theorem 2) is applicable; hence, the center's secret information can be derived by $(n+1)$ user's conspiracy.

Furthermore, Shamir developed a more general attacking method [27] for the modified system such that $(n+2)$ users conspiracy can derive the center's secret information with high probability.

Theorem 3 [27]: The $(n+2)$ users' $i, (1 \le i \le n+2)$ can derive the center's secret information a with high probability.

Proof: when $(n+1)$ users $i, (1 \le i \le n+1)$ conspire, they have the following system of linear congruence's defied by (31)

$$\begin{bmatrix} EID_1 \\ EID_2 \\ EID_3 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ EID_{n+1} \end{bmatrix} \begin{bmatrix} d_1^j \\ d_2^j \\ d_3^j \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ d_n^j \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ s_{n+1} \end{bmatrix} (\mathrm{mod}\ \varphi(N)) \tag{31}$$

$$= D\, d^j (\mathrm{mod}\ \varphi(N)) \tag{32}$$

Assuming that the matrix D includes n linearly independent column vectors over the integer ring, there exist some positive integers $c_i (1 \le i \le n+2)$ such that

$$\begin{bmatrix} EID_1 \\ EID_2 \\ EID_3 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ EID_{n+1} \end{bmatrix} \begin{bmatrix} d_1^j \\ d_2^j \\ d_3^j \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ d_{n+1}^j \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ s_{n+1} \end{bmatrix} - \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ c_{n+1} \end{bmatrix} \varphi(N) \tag{33}$$

Thus equation (33) can be rewritten by the following:

$$\begin{bmatrix} EID_1 \\ EID_2 \\ EID_3 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ EID_{n+1} \end{bmatrix} \begin{bmatrix} d_1^j \\ d_2^j \\ d_3^j \\ \cdot \\ \cdot \\ \cdot \\ d_n^j \\ -1 \end{bmatrix} = - \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ c_{n+1} \end{bmatrix} \varphi(N) \tag{34}$$

$$= D' d^{j'} \tag{35}$$

From the assumption that the matrix D in equation (33) includes n linearly independent column vectors over the integer ring, it follows that the matrix D' is nonsingular over the integer ring (i.e., $\det D' \neq 0$) with overwhelming probability, and thus, we have $a' \neq \pmod{\varphi(N)}$. On the other hand, we have the following system of linear congruence's:

$$D' d^{j'} = 0 \pmod{\varphi(N)} \tag{36}$$

If the matrix D' is nonsingular over Z_N^*, then $d^{j'} = \pmod{\varphi(N)}$, and this contradicts the above results. Thus, the matrix D is singular over Z_N^*, and we have $\det D' = 0 \pmod{\varphi(N)}$ with high probability. Hence, $\det(D')$ is divisible by $\varphi(N)$ with high probability. Furthermore, consider the case where the other $(n+1)$ users among $(n+2)$ conspire, and define the matrix D'' in a way similar to the above. Also, $\det(D'')$ is divisible by $\varphi(N)$ with high probability. Hence, GCD ($\det(D')$, $\det(D'')$) gives $e\varphi(N)$ where e is a small positive integer. By the above procedure, we can evaluate $\varphi(N)$ efficiently. An additional procedure to find the center's secret information is completely the same as attack (Theorem 2).

5. Enhancement of Security and Processing Cost

The center's secret information for the original system in Section II is derived by n users conspiracy. In this subsection, we consider the practical countermeasure for the enhancement of the security of the system. (For simplicity, assume that n = 512 throughout this subsection.) The center partitions a 512-dimensional binary vector B into 256 segments, every two bit, such as

$$\begin{aligned} B &= (b_1, b_2, b_3, \cdots\cdots\cdots, b_{511}, b_{512}) \\ &= (seg_1, seg_2, seg_3, \cdots\cdots\cdots, seg_{511}, seg_{512}) \end{aligned} \tag{37}$$

Then, the center defines $a(i; jk)(1 \le i \le 256; j, k \in \{0,1\}$ appropriately, computes $h(i; jk)(1 \le i \le 256; j, k \in \{0,1\}$,

$$h(i; jk) = \beta^{a(i; jk)} \pmod N \tag{38}$$

for each seg_i, and publishes the table including every $h(i; jk)$ to all users. Furthermore, the center computes each user's secret key s_k by

$$s_k = \sum_{1 \le i \le 256} d^j (i; sge_{ki} \pmod{\varphi(N)} \tag{39}$$

according to equation (13).The entity k's extended identity, EID_k, where EID_k is partitioned into 256 segments, every two bits such as:

$EID_k = (seg_{k1}, seg_{k2}, seg_{k3}, \cdots\cdots\cdots, seg_{k255}, seg_{k256})$.

Then the center distributes it to each user through a highly secure channel.

Encryption

User 2 computes γ_1',

$$\gamma_1' = \prod_{1 \le i \le 256} (h(i, seg_{1i})^{e_i} \pmod N \tag{40}$$

from EID_1 and the published table. User 2 uses γ_1' as γ_1 in the original system (in Section II) to encrypt the message M.

Decryption

This is exactly the same as in the original system in Section II. In the original system in Section II, the center's secret information is derived by 512 users conspiracy, while in the above system it is derived by 1024 (= 4 x 256) users conspiracy. Furthermore, the running cost for encryption-key generation in the above system is about half of the original system. However, the center's public information in the above system is about twice than the original system. Further generalizations, *e.g.*, each EID_i is partitioned into 128 segments every four bits, etc., are possible.

6. Identity-based Key Distribution System

An identity-based key distribution system is a key distribution system based on each user's identity and provides a powerful tool to share common keys in the large-scale telecommunication network. Blom's scheme [28] and Matsumoto and Imai's scheme [29] are known as identity-based key distribution systems without any auxiliary communication, which is a desirable property for common key distribution. (We refer to

such schemes as identity-based noninteractive key distribution systems in the rest of this paper.) In this section, we develop a new identity-based noninteractive key distribution system applying an idea similar to that of the identity-based cryptosystem presented in Section II. Our identity-based noninteractive key distribution system can be regarded as an identity-based version of Diffie and Hellman's key distribution system [4], and the related work can be found in [28,30,31]. The proposed identity-based key distribution system also has thresholds for the number of users required to conspire to compromise the security of the center's secret information. Furthermore, we show a practical modification in light of the secure common key cryptosystem.

6.1. Protocol for Key Distribution

This subsection presents the protocol for the identity-based noninteractive key distribution system. The protocol is composed of two phases; *i.e.*, the first phase is the preliminaries for the center and each user, and the second phase is the procedure for the key distribution between any two users.

1. The First Phase(Preliminaries):

1.1 The center chooses a large prime numbers p and q such that $\varphi(N) = (p-1)(q-1)$ an arbitrary generator β of the multiplicative group of $Z_{\varphi(N)}$. The center also randomly chooses an n-dimensional vector $a = (a_1, a_2, a_3, \ldots\ldots, a_n)$ with the condition $d_l^j = e_l a_l \pmod{\varphi(N)} (1 \le l \le n)$ over $Z_{\varphi(N)}$ and defines $h = (h_1, h_2, h_3, \ldots\ldots, h_n)$ over $Z_{\varphi(N)}$ as $h_i = \beta^{a_i} \pmod{N}, (1 \le i \le n)$ **.** The center makes public N , h and e to all entities, and keeps β , a and d_l^j secret.

1.2 User "i" registers his identity (denoted by ID,) with the center in the form of the binary vector $ID_i = (x_{i1}, x_{i2}, x_{i3}, \ldots\ldots, x_{ik})$ where $k \prec n$ and $x_{ij} \in \{0,1\}, (1 \le j \le k)$ **.**

1.3 For user "i" the center defines an extended ID (denoted by EID_i) in the form of the binary vector EID_i by

$EID_i = (ID_i)^e = (y_{i1}, y_{i2}, y_{i3}, \ldots\ldots, y_{in}), y_{ij} \in \{0,1\}, (1 \le j \le t)$ where $y_{ij} \in \{0,1\}, (1 \le j \le n)$ The center evaluate users i"s secrete s_i by

$$s_i = \sum_{1 \le j \le n} d_l^j y_{ij} \pmod{\varphi(N)}$$

$$= d_l^j EID_i \pmod{\varphi(N)}$$

and issues it to user "i" through a highly secure channel.

2. The Second Phase (Key Distribution): Without loss of generality, we show the protocol of the key distribution between user **1** and user 2. The procedure is basically the same with Diffie and Hellman s scheme [4].

2.1. User 1 generates user 2's extended ID by

$$EID_2 = (ID_2)^e = (y_{21}, y_{22}, y_{23}, \ldots\ldots, y_{2n})$$

And evaluate γ_2 by

$$\gamma_2 = \prod_{1 \le i \le n} (h_i^{y_{2i}})^{e_i} \pmod{N}$$

Note that $\gamma_2 = \beta^{s_2} \pmod{N}$ furthermore; user 1 computes $K_{12} = \gamma_2^{s_2} \pmod{N}$ here, it can easily be shown that $K_{12} = \beta^{s_2 s_1} \pmod{N}$ .User 2 performs a similar procedure and generates $K_{21} = \beta^{s_2 s_1} \pmod{N}$. Thus; user 1 and user 2 succeed in sharing a common key $K (= K_{12} = K_{21})$ without any auxiliary communications.

7. Conclusion

In this paper present the modification in an identity-based beta cryptosystem, security under the generalized discrete logarithm problem with distinct discrete exponents in the multiplicative group of finite fields and integer factorization problem. The proposed scheme satisfies Shamir's original concepts in a strict sense, *i.e.*, it does not require any interactive preliminary communications in each data transmission and has no assumption that tamper free modules are available. This kind of scheme definitely provides a new scheme with a longer and higher level of security than that based on a generalized discrete logarithm problem and integer factorization problem. The proposed scheme also requires minimal operations in encryption and decryption algorithms and thus makes it is very efficient. The present paper provides the special result from the security point of view, because we face the problem of generalized discrete logarithm problem and integer factorization problem at the same time in the multiplicative group of finite fields as compared to the other public key cryptosystem, where we face the difficulty of solving the traditional discrete logarithm problem in the common groups and integer factorization problem.

References

[1] Shamir "Identity-based cryptosystem and signature scheme", Advances in Cryptology: Proceedings of Crypto' (Lecture Notes in Computer Science 196), Berlin, West Germany: Springer-Verlag, vol. 84, **(1985)**, pp. 47-53.
[2] S. Tsujii and T. Itoh, "An ID-based cryptosystem based on the discrete logarithm problem", IEEE Journal on selected areas in communications, vol. 7, **(1989)**, pp. 467-473.
[3] T. ElGmal, "A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE Trans. Inform. Theory, vol. 31, **(1995)**, pp. 469-472.
[4] W. Diffie and M. E. Hellman, "New direction in Cryptography", IEEE Trans.Inform.Theory, vol. 22, **(1976)**, pp. 644-654.
[5] C. Meshram and S. A. Meshram, "An Identity based Beta Cryptosystem", IEEE Proceedings of 7th International Conference on Information Assurance and Security (IAS 2011), **(2011)** December 5-8, pp. 298-303.
[6] E. Okamoto and K. Tanaka, "Key distribution system based on identification information", IEEE J. SeIecr. Areas Commun., vol. 7, **(1989)** May, pp. 481-485.
[7] C. Meshram and S. A. Meshram, "Some Modification in ID-Based Cryptosystem using IFP & DDLP", International Journal of Advanced Computer Science and Applications, vol. 2, no. 8, **(2011)**, pp. 25-29.
[8] W.-B. Lee and K.-C. Liao, "Constructing identity-based cryptosystems for discrete logarithm based cryptosystems", Journal of Network and Computer Applications, vol. 27, **(2004)**, pp. 191–199.
[9] M.-S. Hwang, J.-W. Lo and S.-C. Lin, "An efficient user identification scheme based on ID-based cryptosystem", Computer Standards & Interfaces, vol. 26, **(2004)**, pp. 565–569.
[10] K. Ohta, "Efficient identification and signatureschemes." Electron. Lett., vol. 24, no. 2, **(1988)**, pp. 115-116.
[11] M. Bellare, C. Namprempre and G. Neven, "Security Proofs for Identity-Based Identification and Signature Schemes", Cryptol., vol. 22, **(2009)**, pp. 1–61.
[12] R. C. Merkle and M. E. Hellman, "Hiding information and signatures in trapdoor knapsacks", IEEE Trans. Inform. Theory, IT- 24, **(1978)**, pp. 525-530.

[13] L. Harn, "Public key cryptosystem design based on factoring and discrete logarithm", IEEE Pro. Comput. Digit. Tech, vol. 141, no. 3, **(1994)**, pp. 193-195.
[14] J. Gordon, "Strong RSA keys", Electron. Lett., vol. 20, no. 12, **(1984)**, pp. 514-516.
[15] E. Kiltz and Y. Vahlis, "CCA2 Secure IBE: Standard model efficiency through authenticated symmetric encryption", CT-RSA, Vol. 4964 of Lecture Notes in Computer Science, Springer, **(2008)**, pp. 221–239.
[16] C. Meshram, "A Cryptosystem based on Double Generalized Discrete Logarithm Problem", Int. J. Contemp. Math. Sciences, vol. 6, no. 6, **(2011)**, pp. 285 -297.
[17] C. Meshram, "Modified ID-Based Public key Cryptosystem using Double Discrete Logarithm Problem", International Journal of Advanced Computer Science and Applications, vol. 1, no. 6, **(2010)**, pp. 30-34.
[18] R. Gangishetti, M. Choudary Gorantla, M. Lal Das and A. Saxena, "Threshold key issuing in identity-based cryptosystems", Computer Standards & Interfaces, vol. 29, **(2007)**, pp. 260–264.
[19] J. Sun, C. Zhang, Y. Zhang and Y. Fang, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks", IEEE Tran. On Parall. and Distributed Systems, vol. 27, no. 9, **(2010)**, pp. 1227-1239.
[20] D. Boneh and M. K. Franklin, "Identity based encryption from the Weil pairing", SIAM Journal on Computing, vol. 32, no. 3, **(2003)**, pp. 586–615.
[21] D. Boneh, R. Canetti, S. Halevi and J. Katz, "Chosen-ciphertext security from identity-based encryption", SIAM Journal on Computing, vol. l.5, no. 36, **(2006)**, pp. 1301–1328.
[22] U. M. Maurer and Y. Yacobi, "Non-interactive public key cryptography", Cryptology—Eurocrypt'91, New York: Springer, **(1991)**, pp. 498–507.
[23] U. M. Maurer and Y. Yacobi, "A non-interactive public-key distribution system", Des Codes Cryptogr., vol. 9, no. 3, **(1996)**, pp. 305–316.
[24] Y. M. Tseng and J. K. Jan, "ID-based cryptographic schemes using a non-interactive public-key distribution system", The 14th Annual Computer Security Applications Conference, **(1998)**, pp. 237–243.
[25] C. Cocks, "An Identity Based Encryption Scheme Based on Quadratic Residues", Cryptography and Coding - Institute of Mathematics and Its Applications International Conference on Cryptography and Coding {Proceedings of IMA(2001), LNCS 2260, pp. 360-363, Springer-Verlag, **(2001)**}.
[26] D. Coppersmith "private communication", **(1987)** November.
[27] A. Shamir "private communication", **(1988)** June.
[28] R. Blom, "Non-public key distribution," in Proc. Crypto'82, **(1982)**.
[29] T. Matsumoto and H. Imai, "On the key predistribution system: A practical solution to the key distribution problem", Advances in Cryptology: Proceedings of Crypro '87 (Lecture Notes in Computer Science 293). Berlin, West Germany: Springer-Verlag, **(1988)**, pp. 185-193.
[30] K. Koyama and K. Ohta, "Identity-based conference key distribution system", Advances in Cryptology: Proceedings of Crypto '87 (Lecture Notes in Computer Science 293). Berlin, West Germany: Springer-Verlag, **(1988)**, pp. 175-184.
[31] H. Tanaka, "A realization scheme for the identity-based cryptosystem", Advances in Cryptology: Proceedings of Crypto '87 (Lecture Notes in Computer Science 293), Berlin, West-Germany: Springer-Verlag, **(1988)**, pp. 340-349.
[32] K. Nakamura, E. Okamoto, K. Tanaka and S. Miura, "Private communication", **(1987)** August.
[33] C. Meshram, S. A. Meshram and M. Zhang, "An ID-based cryptographic mechanisms based on GDLP and IFP", Information Processing Letters, vol. 112, **(2012)**, pp. 753–758.
[34] C. Meshram and S. Meshram, "An identity based cryptographic model for discrete logarithm and integer factoring based cryptosystem", Information Processing Letters, vol. 113, **(2013)**, pp. 375-380.
[35] C Meshram, "An Efficient ID-based Cryptographic Encryption based on Discrete Logarithm Problem and Integer Factorization Problem", Information Processing Letters, vol. 115, **(2015)**, pp. 351-358.
[36] C. Meshram, X. Huang and S. Meshram, "Constructing Identity-based cryptographic scheme for QER cryptosystem", International Journal of Pure and Applied Mathematics, vol. 81, no. 5, **(2012)**, pp. 737-753.
[37] C. Meshram, X. Huang and S. Meshram, "New Identity-based cryptographic scheme for IFP and DLP based cryptosystem", International Journal of Pure and Applied Mathematics, vol. 81, no. 1, **(2012)**, pp. 65-79.
[38] C. Meshram, S. Meshram and C. Ram, "Constructing identity-based cryptographic scheme for beta cryptosystem", International Journal of Applied Mathematics", vol. 25, no. 5, **(2012)**, pp. 609-624.

Authors

Dr. Chandrashekhar Meshram, he received the M.Sc and M.Phil degrees, from Pandit Ravishankar Shukla University, Raipur (C.G.) in 2007 and 2008, respectively and PhD from R.T.M. Nagpur University, Nagpur (M.S.) India. Presently he is teaching as an Assistant Professor in Department of Applied Mathematics, Gyan Ganga Institute of Technology and Sciences, Jabalpur (M.P.), India. His research interested in the field of Cryptography and its Application, Boundary value problem, Statistics, Raga (Music and Statistics), Neural Network , Ad hoc Network, Number theory, Environmental chemistry, Mathematical modeling, Thermo elasticity, Solid Mechanics and Fixed point theorem. He is a member of International Association of Engineers (IAENG), Hong Kong, World Academy of Science, Engineering and Technology (WASET), New Zealand , Computer Science Teachers Association (CSTA), USA, Association for Computing Machinery (ACM), USA, International Association of Computer Science and Information Technology(IACSIT), Singapore, European Association for Theoretical Computer Science (EATCS), Greece, International Association of Railway Operations Research (IAROR), Netherland, International Association for Pattern Recognition (IAPR), New York , International Federation for Information Processing (IFIP) ,Austria, Association for the Advancement of Computing in Education (AACE),USA, International Mathematical Union (IMU) Berlin, Germany, European Alliance for Innovation (EAI), International Linear Algebra Society (ILAS) Haifa, Israel, Science and Engineering Institute (SCIEI), Machine Intelligence Research Labs (MIR Labs) , USA, Society: Intelligent Systems, KES International Association, United Kingdom, Universal Association of Computer and Electronics Engineers (UACEE), The Society of Digital Information and Wireless Communications (SDIWC) and Life –time member of Internet Society (ISOC),USA ,Indian Mathematical Society , Cryptology Research Society of India and Ramanujan Mathematical Society of India (RMS) and editor in chief of IJRRWC, UK and managing editor of IJCMST, India. He is regular reviewer of thirty International Journals and International Conferences.